HIT Policy Committee
Privacy & Security Policy Workgroup
Draft Transcript
April 26, 2010

Presentation

Judy Sparrow - Office of the National Coordinator - Executive Director

Good afternoon, everybody and welcome to the Privacy & Security Policy Workgroup. This is a federal advisory call, so you will have opportunity at the end of the meeting to make public comment. I'll do a roll call now. Devin McGraw?

Deven McGraw - Center for Democracy & Technology – Director

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director

Latanya Sweeney? Gayle Harrell? Paul Tang? Mike Klag? Judy Faulkner? John Blair?

John Blair – Tacanic IPA – President & CEO

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director

Paul Egerman?

Paul Egerman – eScription – CEO

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director

Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director

Paul Uhrig? Dave Wanser?

Dave Wanser – NDIIC – Executive Director

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director

Kathleen Connor?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director

Rachel Block? Laurel Stein? Terri Shaw? John Houston?

John Houston – Univ. Pittsburgh Medical Center – VP, Privacy & Info Security

Here.

Judy Sparrow - Office of the National Coordinator - Executive Director
Joyce DuBow? Joyce said that she'd be late. Mike DeCarlo?

Mike DeCarlo – BlueCross BlueShield
Here.

Judy Sparrow - Office of the National Coordinator - Executive Director
Connie Delaney?

Connie Delaney – University of Minnesota School of Nursing – Dean
Here.

Judy Sparrow - Office of the National Coordinator - Executive Director
Marianna Bledsoe?

Marianna Bledsoe – NIH – Deputy Associate Director
Here.

Judy Sparrow - Office of the National Coordinator - Executive Director
Peter Basch? Adam Green?

Adam Green – Progressive Chain Campaign Committee – Cofounder
Here.

Judy Sparrow - Office of the National Coordinator - Executive Director
Did I leave anybody off?

Sarah Wattenberg – ONCHIT – Public Health Advisor
Sarah Wattenberg.

Judy Sparrow - Office of the National Coordinator - Executive Director
All right.

Jodi Daniel – ONC – Director Office of Policy & Research
Judy, this is Jodi Daniel. I'm on.

Judy Sparrow – Office of the National Coordinator – Executive Director
Oh, good.

Carl Dvorak – Epic Systems – EVP
Carl Dvorak joining for Judy Faulkner.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thanks, Carl. Deven, I'll turn it over to you.

Deven McGraw - Center for Democracy & Technology – Director
Okay, terrific. We have, as usual, a packed agenda today and we're going to try to accomplish a couple of things. One is to spend a bit of time right in the beginning of this call talking about whether we want to make any recommendations to the policy committee on the permanent certification rule notification of proposed rule-making and its treatment of the Privacy & Security certification criteria as applied to EHR

modules. You'll recall that it's essentially the same criteria that was in effect for the temporary certification program rule, but the comment deadline for the temporary rule was a very fast one, we were not able to have a full discussion on our call, and the comments that we did submit reflected the thoughts of a few of us but not necessarily the whole workgroup.

So you'll recall that on a previous meeting of our workgroup I committed to allowing us to take another stab at this to incorporate some views of folks that we were not able to hear more fully from the first time around because of the very short time frame. So I wanted to do that in the beginning of the call today, and then we'll follow on with a continuing discussion of the role of consent in one to one exchange when intermediaries are used and see how much further we can get with that using the discussion framework that you should have gotten in an e-mail from Judy on Friday.

Rachel Block – New York eHealth Collaborative – Executive Director
Deven, it's Rachel. I just wanted to let you know I joined.

Deven McGraw - Center for Democracy & Technology – Director
Thank you. Did anyone else join in the interim after roll call? Okay. I'd like to –

Judy Faulkner – Epic Systems – Founder
Deven, this is Judy. I joined too.

Deven McGraw - Center for Democracy & Technology – Director
Okay, great. Thanks, Judy. Anyone else on mute that didn't weigh in? Okay, then I'd like to turn it over to Paul Egerman just to give us a sense of what process there might be to getting the policy committee to consider something if we are so inclined to make a recommendation and also pass on any words of wisdom that he might have. Paul?

Paul Egerman – eScription – CEO
Thanks, Deven. I feel under pressure to say something that is a word of wisdom, however, I'll do my best. First, in terms of the process, Deven, as you correctly said, the comments on the temporary program were due April 9th and this workgroup did make some comments that were approved by the policy committee, and so I assume were submitted to David, to the National Coordinator. For the permanent program, the process itself is pretty much the same. The comments are due May 10th – I think it's May 10th, it may be May 9th, May 9th or 10th – and if this committee wants to make any comments then we can and then Deven will take it probably to a telephone conference call of the policy committee to get them approved and then it happens. In terms of the process itself, we're focused on a lot of issues with privacy and security, but the certification NPRM really is very important because this is where the rubber meets the road. This tells us really how the whole thing is really going to get done and so the other comment I make is it is an important thing.

Now, the permanent program for privacy and security really repeats the same thing it said in the temporary program, so you have these concepts that modules can be submitted as a bundle if the bundle represents a complete EHR, and the bundle would be tested against privacy and security without testing the individual modules. So that's sort of like a carve-out for modules. There are two other carve-outs. One carve-out is basically if a module actually does a security or privacy function by itself, so if the module is say an encryption module, then it's really clear that you test it for encryption but you don't test it for anything else. The third carve-out is whether or not a module can prove that it's technically infeasible to test it for certain privacy and security issues. The only example I can think of off the top of my head is if somebody has a module that does a calculation or maybe is a nice way to enter data that never stores any data, then maybe you'd say there's no reason to test it against encryption because it's not really storing any data.

So we made a comment on all of that stuff last time on the temporary program and if we want we can simply repeat our comment for the permanent program, or if we want we can change the comment. The other places where if we want to we can comment is in the permanent program those issues about surveillance and decertification, so surveillance is the certification bodies have to watch to see if vendors really do what they're supposed to be doing with certification. If we want to make any specific comment as it relates to privacy and security on surveillance we can, and we can also make a specific comment on decertification.

Deven McGraw - Center for Democracy & Technology – Director

Thank you, Paul. That's very helpful. The set of comments that was submitted last time admittedly wasn't done with full input because they had to base it on e-mails that came in, and so we largely looked at the one exception for bundled EHRs that had to do with whether there was a particular functionality that was done off site or not under the direct control of the rest of the bundle, this is for the bundled exception, and it just was something that at least a couple of folks on the workgroup called out to say I don't understand what this exception deals with and either they're bundled together or they're not. And we added some provisions on labeling that were consistent with those of the certification workgroup so that it came as a complete package.

Once again, we don't have the opportunity to comment just as our workgroup, and so essentially what we need to decide on this call is whether we're going to suggest something to the policy committee, which would then be considered in a policy committee phone call so we can get this done in time to submit it officially to David in his capacity as Health IT National Coordinator as part of the comments on the rule.

I know, Dixie and Kathleen, I'm calling on you now only because I know I heard from you all in wanting to take another stab at this. So I hope I'm not putting you on the spot, but I wanted for the other members of the workgroup to get a chance to hear what your concerns were particularly with the privacy and security criteria for the EHR modules. Again, I think we can comment on some other stuff too, but that one seems most up our alley given our scope and purview of the workgroup.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

Hi, this is Kathleen. My question on the question that was put forward as a comment about what do you do when you have a bundle of modules that are … to complete EHR but one or more of these modules is software-as-a-service, for example, that is not completely under the control of the vendor that's putting this bundle forward for certification. What I wasn't clear about is if you look at the tests that are out on this site it seems to me that this entire bundle would have to pass the certification test for the security criteria in order to get the label.

So I wasn't sure what the concern was, other than perhaps a concern that maybe down the road the software-as-a-service type module entity that has control over what it does about these security criteria could change over time and that the vendor would not have control on keeping that original certification. But I think that's addressed by some of the things around if a module or bundle of modules has changed down the road then certification has to be looked at again in some way. The lack of clarity there, it would be really helpful to get the concerns stated and maybe there's ways to approach it, like making sure that if there's changes in the modules down the road it gets looked at again, or some kind of provision like that.

Deven McGraw - Center for Democracy & Technology – Director

To be honest, Kathleen, essentially I couldn't understand the comments that I did receive from workgroup members, and that frankly were the comments that occurred to me is that I didn't understand the exception to the exception. So either it's presented as a bundle or it isn't. What the significance was of well, if it's presented as a bundle but some piece of it isn't under direct control, I didn't understand why ONC would call that out as an exception to what would otherwise be presented as a bundle and why would it matter where it's located and under whose control. Are we essentially saying the same thing, or am I missing something?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

No, I think we're actually saying the same thing. I guess the best thing we can do is request clarification and maybe put a little bit about why this is unclear. I think you did that, but I just didn't see why you'd call it out.

Deven McGraw - Center for Democracy & Technology – Director
Yes, why I called it out was I couldn't figure out why they called it out.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I did mean them, not you.

Paul Egerman – eScription – CEO
This is Paul Egerman. I agree with what was just said. It was odd that they have the exception to the exception. The only thing I can think of is that they have an underlying theory that software-as-a-service requires some additional security or privacy test, that's the only thing. But if that's the case they should just say that affirmatively, as opposed to doing it this way.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I guess we'd have to think about what kind of impedance that might be for vendors trying to put these bundles forward. It may not be a big problem because if you are a software-as-a-service vendor for a particular module and you want to assert that it conforms to this criteria, that it's providing encryption or some such thing, you may have already gotten it certified and then when it's pulled together with the rest of the modules the vendor of the bundle is demonstrating that that software-as-a-service module indeed works well with the rest of the modules.

Paul Egerman – eScription – CEO
That's exactly right. Your comment is a good one. The purpose of the label is to say though if you submit this part of a bundle that does not mean that the module itself has passed the certification process. In other words, the module isn't allowed to say it is certified if it was submitted as a bundle unless it submits itself individually as a module.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
My concern was different. This is Dixie Baker.

Deven McGraw - Center for Democracy & Technology – Director
Okay, Dixie, go ahead.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I do understand, I don't want to be misinterpreted, I do understand why they would want to say that we want to leave systems integration as a responsibility of the eligible professional or hospital. I do understand that except when it comes to security. The reason I think security is an exception is that you can't have security across an enterprise, a security policy enforced consistently across an enterprise through that approach. If you have a set of EHR modules, each of which has been independently certified, you either will have every module implementing security functionality, in which case you'll have inconsistent policy enforcement across the enterprise, or you'll have one or more of those modules assuming that somebody else is providing the security.

I feel that it's very reasonable in the case of security to require that a module that's submitted for certification as an independent module be required to specify its assumptions regarding the security requirement certification criteria, specify their functions, and secondly, completely specify the interfaces to external security services. Or if the module is a security module, that it completely specify the interfaces for providing those security services to other modules. I think that that's completely reasonable requirements.

Deven McGraw - Center for Democracy & Technology – Director
Dixie, I think I understand that. Again, I think the wording of the NPRM is that they have to satisfy all of them, that's the default.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, but that's not a good thing. If every module satisfies every one of them and you put those modules together, then every one of them could each be enforcing a different security policy or enforcing the security policy differently. For example, a user could have a different identity in every single module and what kind of accountability of disclosures are you going to have if you can't trace an individual user across modules. Security is something that needs to be implemented at an enterprise level, not at an individual module level.

Paul Egerman – eScription – CEO
Your comments are very interesting. It seems to me if I'm hearing it right, maybe I'm not, that what you're really commenting on is situations where modules are not submitted as a bundle, where somebody's just submitting a module by itself.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I agree with the statement that if a set of modules are submitted as a bundle that it be evaluated as a complete EHR. I think that's completely reasonable without the exception.

Deven McGraw - Center for Democracy & Technology – Director
The exception to the exception.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, yes. That's fine. I would consider that a complete EHR as well.

Paul Egerman – eScription – CEO
So you've got a different category of comments, so rather than talk about the bundling and exceptions you have a comment that when a module is submitted by itself as a module.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's really the only concern I have is if it's submitted as an independent module, yes.

Paul Egerman – eScription – CEO
And part of its certification requirements should be that it has to describe any assumptions or interfaces it needs to security services.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
And, assumptions and interfaces. I think that that makes more sense than allowing a module to do everything itself independent of all the rest of the systems.

Deven McGraw - Center for Democracy & Technology – Director
But does that get to the question of the interoperability question, Paul, that you all highlighted in the certification workgroup letter, which is you can't test for that, so it's a module problem that isn't limited just to security arguably, although one could argue that the issues that it raises are most acute in that context. But essentially anybody who's going the modular route is going to be on their own in terms of whether all the parts work together. And in the security context that means on their own as to whether the audit functionality, for example, that's in one module essentially picks up the transactions that are taking place in the other modules. That's an example.

Paul Egerman – eScription – CEO
That's right. Deven, your comments are correct. The issue with what Deven is suggesting is that it would be like what I would call certification criteria, but it would not be testing criteria. In other words, there's no way you could test to see whether or not what was said was accurate, this would just be a statement that presumably you would require as part of labeling or something that people would have to do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

I would require that the interfaces be tested.

Paul Egerman – eScription – CEO
But there's no way to test them.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, you could have them submit with the modules an example of a component that it could interface with.

Paul Egerman – eScription – CEO
Yes, but it's the same thing, there's no way to test it. There's no testing criteria that was approved in the IFR for doing this. So they don't have any testing criteria or test process in place; all you can do is submit information. There's nothing wrong with that per se, that's just an observation to make sure people understand what it is you're proposing.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I totally agree with Dixie about the issue. I think it's possible for the final rule to at least describe the standards that you're using for your privacy and security modules. But as to testing, perhaps that's something that vendors can do on their own just to enhance the value of what they're offering to the market. There are bodies that can do that or they can do that with partners and add that to the label on a voluntary basis too. That's another approach.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I can see where even if they submitted one product, this is the product that will test our interface, if it were a proprietary interface that wouldn't be good either. So yes, I can see your point, yes. But I think that requiring them to completely specify, especially in a services oriented architecture specifying an interface is quite common and I don't think that that would be an unreasonable requirement.

Deven McGraw - Center for Democracy & Technology – Director
What do folks think about that? This is one of those tricky areas. Dixie, when you first brought this to my attention I wondered whether the inability to test interoperability, at least at this stage, makes the EHR module route a very tricky one for providers, quite frankly. But it's out there and one can see that there are reasons for it, but I think it does pose particular challenges in this space.

Judy Faulkner – Epic Systems – Founder
I think it makes sense to check at least one, because then you can see whether it's possible. If nowhere can it be done, if they can't find one to test, all you know then is it's possible. You don't know whether it's used that way everywhere. I think it makes sense to test it, though.

Paul Egerman – eScription – CEO
My concern is that I don't think they have a mechanism to test one.

Judy Faulkner – Epic Systems – Founder
Yes, I understand what you're saying. Then we develop a mechanism to test it.

Paul Egerman – eScription – CEO
Well, the problem is that the test mechanisms are all set up in the IFR and so what you could do is you could ask them to submit an example of one for Dave testing it, I suppose. It would be nice to test it, but it's exactly as Deven says an interoperability problem. I think it's hard to do.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Why is it any harder than testing against any other certification criteria? We have, what, seven or however many, certification criteria in the IFR that are around security, so you test it against those criteria.

Paul Egerman – eScription – CEO
The reason it's harder, Dixie, is those seven are already spelled out in the IFR and the test scripts and test procedures have been written for that. So if I've got a module, maybe I've got a module that tests eligibility, you can't just create a new security … interface.

Judy Faulkner – Epic Systems – Founder
Are you saying, Paul, that that's the sum total and no more can be added to that?

Paul Egerman – eScription – CEO
That's my understanding. It can't be added unless it goes through that whole IFR process.

Deven McGraw - Center for Democracy & Technology – Director
Yes, that's right. It doesn't mean that in future certifications that couldn't be improved, but –

Mike DeCarlo – BlueCross BlueShield
That's my question here, in the permanent program where they're splitting the testing function and making that the purview of NIST and then the certification function of course is going to be the purview of the ACB, are we saying that the certification body could do as a certification function some additional testing, or is that out of their purview as well?

Paul Egerman – eScription – CEO
My understanding is that it's out of their purview, it's not included for this purpose. Remember, NIST doesn't do the testing. NIST really accredits the testing laboratory to make sure that the laboratories are doing the right stuff. So the testing labs do the testing.

Mike DeCarlo – BlueCross BlueShield
Within the confines of the criteria in the IFR.

Paul Egerman – eScription – CEO
Yes, that's the way I understand it. Somebody can tell me if I've got it wrong. I might not be 100% right on this.

Deven McGraw - Center for Democracy & Technology – Director
No, I think you're right, Paul.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's the right model.

Deven McGraw - Center for Democracy & Technology – Director
So essentially what we'd like to be able to do is require these modules to be tested against one another as part of achieving certification in the permanent program. So without the criteria against which to test we could do a number of things, encourage the development of such criteria so that in later certification rounds it can be included, if that makes sense, and in the meantime requiring the entities to at least, as Dixie said, attest to assumptions in interfaces to external security services. Dixie, I'm not sure I fully grasp what that ought to look like in prose, so I may lean on you to help me with some drafting, but I get it at a top of the trees level. It's like if we can't independently test it and vet it we can at least at a minimum in the early stages ask the vendors of these modules to say how they work with the security components that ultimately all should be present.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences

Let me tell you exactly, what I actually recommended was three things. The list of assumptions about the privacy and security attributes. A description of how each of the privacy and security certification criteria can be met in the assumed environment. And third, a specification of each of the interfaces …. Now, as Paul and you guys are talking it occurs to me that if we took the approach that Judy suggested, maybe they bring in some component that's to be tested with, and let's say it fails then whose fault is it? I almost think that in this case it should be an analytical function, an examination of the completeness of the interface specifications and not a test.

Deven McGraw - Center for Democracy & Technology – Director
I'm not sure that there's any meaningful distinction. Don't you still run into the same problem we're talking about, is that we don't have any criteria in the IFR to –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, yes. I happen to think that if there's testing you would test against the criteria that are there.

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But I would agree with you, if you're evaluating the completeness of a specification of an interface, then we have no criteria for that.

Deven McGraw - Center for Democracy & Technology – Director
Not yet. We'd like some criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that would be good.

Mike DeCarlo – BlueCross BlueShield
I'm looking at the IFR now, they failed to adopt Table 2B as criteria under 170-300 series. That's the problem, isn't it?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
What's Table 2B? Is that the—

Mike DeCarlo – BlueCross BlueShield
Table 2B is the one that's adopted privacy and security standards.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's all in the preface. That's not in the—

Mike DeCarlo – BlueCross BlueShield
That's not in the actual …, yes, they—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The only standards they actually adopted was … 1.

Mike DeCarlo – BlueCross BlueShield
Right, so they can't really give full force and effect now to the certification criteria, which says that they have to be tested against privacy and security certification criteria adopted by the secretary because they failed to do that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
They did adopt the criteria. They adopted the criteria, the certification criteria in the body of the regulation; they just eliminated the specific EGs that are in Table 2B.

Deven McGraw - Center for Democracy & Technology – Director
Right. So in some cases, for some of the criteria there are not specific technical standards that have to be met, but the functionality has to be present.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, exactly. When we came back the standards committee we did recommend that they add AES as a standard, but even then it would just be …1 and AES, those would be the only two standards.

Mike DeCarlo – BlueCross BlueShield
I'm wondering if there's a simpler way to address this issue. I'm thinking about what you're suggesting, Dixie, which is interesting. But we've also got this issue that a module vendor could say that it's technically infeasible to test their software against some security or privacy criteria. So maybe another way of doing this to simply say if you're submitting a module you're either going to get tested against everything or you've got to explain why it is technically infeasible to not get tested against something, or you've got to explain how you're going to accomplish that functionality through interfaces or other means.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that's exactly what I recommended.

Mike DeCarlo – BlueCross BlueShield
So you take the infeasible thing and you simply expand it to you're going to get tested against everything, you're going to say it's infeasible, or you're going to say how you're going to accomplish it through basically an interface with other services that provide that same functionality.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Paul, when we actually submitted our first comments, our first recommendations were that, and this was against the IFR, not the certification criteria, was to make each of the security certification criteria addressable in the same way that HIPAA uses addressable, which is exactly what you're saying. So that every vendor that submitted an EHR module would have to either say, my product does this, meets this certification criteria, or it would explain why it doesn't make sense and explain how that functionality, they're assuming how that functionality would be provided along with the interfaces, etc.

Deven McGraw - Center for Democracy & Technology – Director
I'm less inclined to use that analogy, only because addressable to me in the security rule context is not about whether it's technically infeasible, although that's certainly an excuse for doing so, but to me it's more about well, I know I need to protect this data so either I have to do this or I have to do that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I agree. It's—

Deven McGraw - Center for Democracy & Technology – Director
…exactly the right analogy. We certainly did say, at least in our meetings use comments that the meaningful use, quite frankly, of those security criteria that are in the IFR, they really are, most of them, addressable provisions and the providers really have to do that and OCR should consider whether they need to be eased into requirements now that the technology is out there and widely available.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and also I would add to your argument here that the term has taken on its own life. You're right, it's probably not a good term to use, but the approach that Paul is describing is exactly what we recommended. You either do it, or you explain why not and what compensates for it.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I think that the piece that is missing, I think essentially that's what the rule says, it's explaining how you compensate for it is the piece that's missing.

Carl Dvorak – Epic Systems – EVP
I'm wondering, the goal is ultimately that a health care provider would be able to use these modules in concert to meet the requirements, what if the module provider said they couldn't test for it, what if they had to instead provide a written statement as to how a customer using that module would be able to meet that requirement in a formal manner so that the customers could collect up those statements from the module providers and use that as a mechanism for accountability. So that if they bought five modules that claimed to help meet the requirement, although they couldn't test for them that they could at least have something binding with those module providers to make sure that they really could put those pieces together and make them work.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
That's what an interface spec would do. That's exactly what we're talking about doing. If they had to complete interface specification and then they hooked it up to an audit component and it didn't audit.

Deven McGraw - Center for Democracy & Technology – Director
I think you have to think, though, about how this is likely to work in practice. Unless it's a homegrown piece of software, the vendor of a module is the one who's going to submit it for certification. To the extent that there are any eligible providers or hospitals that are going to want to cobble modules together, it ends up not falling on the vendor, and this has been true all throughout the certification IFR, it falls on the brave person who decides that the way they want to pull this together is by pulling modules together. Essentially as long as what they're purchasing in module is certified, they get federal funding for it and there isn't any mechanism at the end of the day for saying, well, did you get all of the parts together.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and that's—

Deven McGraw - Center for Democracy & Technology – Director
Where is it, period?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Deven McGraw - Center for Democracy & Technology – Director
There are consequences of that across the different categories of meaningful use, but where it falls I think the most unfortunate is in security, where you can essentially be missing a piece that I think we all intended would be there, because it's not covered by a module. But in the meantime you've got everything else.

Paul Egerman – eScription – CEO

But the other practical reality too, though is that you can still have all the functionality that's required and the customer could choose to implement none of it, which is—

Deven McGraw - Center for Democracy & Technology – Director
That is absolutely true.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Then it's … the vendor's fault.

Mike DeCarlo – BlueCross BlueShield
No, it's not the vendor's fault, but what I think happens here is just that, though. You see a lot of functionality that goes by the wayside very quickly at implementation, whether it be functionality related to security or not. That's the other issue with meaningful use is just because you lead a horse to water.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I totally agree. But getting back to this set of comments, if it's the individual EHR module vendors, if all I'm selling is encryption software and I present it and it meets the certification criteria and I get my label and it says, this only does X and is certified to do X, why would it be my responsibility to say how it interfaces with other products.

Mike DeCarlo – BlueCross BlueShield
That's right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Well, it would be your responsibility to specify how your service can be accessed by the other products.

Paul Egerman – eScription – CEO
That's right, too, Dixie. First, let me give an example. Suppose you have a module that does eligibility checking, you might say well, that module really shouldn't be tested against anything that checks for valid user identity, because it's going to be embedded into another product, it's going to be called by something that already tested user identity. I use that as my example. So the way I'm suggesting that we respond to your concern, Dixie, is just with a very broad statement that says that EHR modules should be tested against all privacy and security unless they can show it's technically infeasible, or unless they can describe how that functionality is already achieved by the module through some other purpose. So again, the example I gave with the eligibility thing, the assumption is that the module doesn't interact with users directly and as a result that's the reason why it doesn't have to have the user identification protocols.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I would not accept it's technically infeasible because I would require that it's either tested against everything — if it's a component I don't want it to do everything. If a component isn't designed to be integrated with other products, I don't want it to do all the security functions, you know? You don't want every single module independently doing security. I think that every product should be submitted with here are my assumptions about my environment, this is kind of how common criteria are done, here are my assumptions about the environment and here are my interfaces for the security functions that are required for certification.

Deven McGraw - Center for Democracy & Technology – Director
Except that module if it's only doing one thing, why would we hold it responsible for how all of the rest of it is going to get done?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
You wouldn't. You would say, what are your assumptions? It would go, here are my assumptions. I assume that this module is going to be deeply embedded within another module and that that module will be responsible for security.

Paul Egerman – eScription – CEO
Dixie, instead of saying technically infeasible, what you are recommending or suggested is the module should describe the reasons and assumptions that cause it not to be tested against various security criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. In fact, there are common criteria for trusted systems has, here's how you specify your assumed operational environment. I think that they should specify here's my assumed operational environment. And assuming this environment, here's how these security criteria would be met.

Deven McGraw - Center for Democracy & Technology – Director
I'm not disagreeing with you, Dixie, but I guess I'm suggesting that if in fact I'm the manufacturer of a module that just does one thing, that I'm struggling to see why I have to – and I give assumptions as to why the other criteria are inapplicable, why I would then have to say the products that it would interface with when that's not what I'm selling. I'm selling a module that performs a particular function because of the particularities of that function it shouldn't have to meet certain security criteria that are just completely an anathema, that don't make any sense for it to perform, what's the—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, it wouldn't have to perform, but even if you had a module that did one thing, if that one thing required that that module run with privilege and could undermine the entire security … of the entire environment, I would want to know that.

Deven McGraw - Center for Democracy & Technology – Director
Yes, but I think that that's – and maybe it's specific to modules where part of the assumption, part of the environment you're assuming is that there will be other pieces that will perform other functionalities that will have to work together.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes. They're not going to have a module that just sits there and does nothing and doesn't interface with anything else. It's not going to happen. Even with the operating system it's got to be called by the operating system. It's not going to be a brick.

Deven McGraw - Center for Democracy & Technology – Director
Let me see if we can work up some language that captures what we've had on the call here. I always have a note taker, by the way.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, good.

Deven McGraw - Center for Democracy & Technology – Director
Yes. I know ONC staff often take notes and I try to, but I actually have someone here on my own staff that takes copious notes.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Before we go off this topic there was some discussion a bit back about how it wasn't clear that providers would have to utilize all of the security capabilities in order to meet meaningful use …. It wasn't quite my understanding. If I have an EHR bundle of modules that have passed certification that I intend to use for meaningful use, doesn't the conducting of a risk assessment and remediating any gaps going to require the provider to at least exercise these capabilities? They all work together and they're all important for meeting the security requirements under HIPAA considering whether they're addressable or not. So it does seem that there's some exercising of this capability.

Deven McGraw - Center for Democracy & Technology – Director
Yes, that's a good point, Kathleen. That's a very good point that I hadn't thought of. I think I had a vision of a check list of features and functions that you wouldn't get your check from Uncle Sam unless you could check off every single box. Essentially, I think you're right, that the way that that happens in an EHR module type of circumstance, not to mention that there's … issues and general compliance that … security …. I don't think we need to worry about that so much. I think that if a security module doesn't integrate well with other ones it will become really obvious during that exercise.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Yes, if it doesn't play well with others.

Deven McGraw - Center for Democracy & Technology – Director
Okay, well let's see, I'll work with Paul to figure out when we might be able to get this in front of the policy committee and I'll work on some language and get it out to you all to look at before we would have to go to the policy committee. It might be on a very tight time frame, like a 24 hour turnaround, but it won't be long.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
We'll watch for it. Thank you.

Deven McGraw - Center for Democracy & Technology – Director
All right, moving to the next item on the agenda, which is continuing our discussion about – I've labeled this "Recommendation on Trust Framework and Consumer Choice for Exchange." For those of you who were either at the policy committee or who listened in, we did give a little report on what we had been discussing and where our thinking was coalescing and what we were struggling with. At the policy committee meeting last Wednesday we of course didn't make any specific recommendations because we're still working on those. We did get some feedback from the policy committee that was interesting. It was reported on in the trade press a bit.

I don't know that we got a whole lot of clarity on the question we started to grapple with in the last meeting, which is what is it about one to one exchange where there's an intermediary involved in facilitating it that sort of morphs it from something that makes us relatively comfortable and seems largely consistent with consumer expectations, into one that crosses over into models that are less expected by the consumer and where we would want to have more stringent privacy and security requirements, which might also include an enhanced role for consumer choice, such as opt-in or opt-out of an HIE, for example, as we saw in the consent paper that ONC commissioned.

So what I've done here, with some help actually from some of the folks that are working on the technical specifications for … direct, in terms of the gradations of what intermediaries are likely to do in the middle in terms of what data that they might have access to. These didn't come completely out of my head, I must confess, which is a good thing, because this is a complicated area but it is actually consistent with some of the discussions that they've been having on the technical side, which makes it all the more important that we be thinking quite quickly actually about what the policy environment is for these scenarios and where it ought to be in terms of what types of recommendations we might want to make.

So I started this discussion guide with a section that I called "Assumptions." The way I really ought to have framed this is conditions that under gird our recommendations, i.e. again, the recommendation that has been on the table with respect to one to one exchange for stage one of meaningful use and our initial recommendation, again, not fully blessed by the policy committee and not fully put before them, but where our thinking has been to date is that with respect to stage one of meaningful use when you have one to one exchange that current law of course applies and we don't need additional consumer consent on top of that. Where we have been tripped up is when you have still direct exchange, still talking about stage one of meaningful use, but there's an intermediary that is facilitating that transport and what is that intermediary's access to data and when does that cross over, again, into this area where we have less comfort.

So the condition I think that under girds that recommendation is that the stage one criteria involves sending data to consumers or patients, that when the data exchange is done with patients it's done with full patient choice. For example, if the patient wants it sent to a PHR it's the patient selected PHR and not a PHR that isn't necessarily one that the patient has requested. In some respects we assume that the business associate rules would apply to entities that receive protected health information from a covered entity to perform a function on their behalf, and I sent around to folks a snapshot of these current business associate rules that was prepared by Adam Green from the Office of Civil Rights, which is very helpful.

We can talk about where that business associate relationship gives us some confidence and where it breaks down. But I wanted to put in there a set of assumptions that that would exist in some way, shape or form. In part because we know that at least with respect to health information exchanges, as a noun, that the high tech act did say that they are business associates when they're exchanging data that's provided by a covered entity, but I think we still don't know what the full meaning of those provisions are because we're waiting for the rule that is pending now in clearance on that issue. Of course it assumes that current federal and state laws apply. We are not trying to change current law in any way in this regard.

When we're thinking about one to one exchange we're thinking of a scenario where it is essentially sent from and thereby vetted by the data holder. It's the push model, but I don't use the word push anymore because it's not necessarily a good description of the technology, but that's essentially I think when we say direct exchange what we're talking about.

I'm also assuming that we're talking about individually identifiable information. We had a lot of discussion on our last call about issues involving de-identified data. It is absolutely an issue that's on our work plan, but I want to parking lot it because we're not going to be able to take all of this in one set of recommendations, we're going to have to knock some of this out over a period of time. And we are again trying to start with a broader approach to consent in exchange, and I think if we stick with individually identifiable health information and get some recommendations out on that piece we can move to de-identification and also to choice at the more granular level, such as by data type. There was some discussion at the policy committee about that issue, but we know that ONC is working on a paper involving, for example, data segmentation and choice down at a granular level. I also will share with you towards the end of our call here today, some plans that we have in the works to do some exploration on the technical feasibility of consent applied at that granular level.

But I wanted to take those off the table, not permanently, but stick them in a parking lot so we can have a very focused discussion on, again, one to one exchange recommendations. The next five examples on here essentially are a gradation which begins with no intermediary in the middle, which I'm not sure it really exists anywhere because the data doesn't move by magic. Even if it's just vendor assisted there's still an entity that's involved in moving the data from point A to point B per the data holder's request, and then it progresses to much more what I call robust intermediary involvement with protected health information.

I think there are a number of things to talk about here. One is, where does the comfort level with one to one exchange involving an intermediary break down and lead us to wanting to have even more stringent policies, including potentially giving patients a greater role in consent. And even with respect to the use of an intermediary, where we're not necessarily saying that there should be any additional consent, I think we certainly need to talk about data access and use and retention policies with respect to the data that is accessed by intermediaries, even when the functions that they're performing are arguably just related to the transport and some minimal access regarding their own business operations, and then you can see it layers on top until you get to higher levels of functionality.

Business associate agreements could be one way of regulating that intermediary use of data, but there could be some issues there. I received some comments from some of you over the weekend on the discussion guide about how in the context of an HIE the power dynamic is likely to be with the HIE, which is the business associate versus the covered entity, in terms of dictating those concerns, and also whether we're comfortable that a business associate agreement would have the limitations on data use that we might want to impose and whether there ought to be another mechanism for being very clear and limited with respect to intermediary's use of data. Notwithstanding that there could be in many cases a whole chain of organizations involved in the transport process involving multiple BAAs down the channel, which is again something that I think we need to think about.

Essentially, because I tried to lay this out as a straw man and this is thinking from Rachel and I, and so we definitely want some feedback, but essentially with respect to scenarios one, two, and three, and even for me it extended to number four, I did not see that there was a policy need for requiring additional patient consent. But I saw a strong policy need for being very clear about how the intermediaries could access and use and to what extent could they retain the data that they may have access to by virtue of the transport, so whether that's in metadata, which is essentially the routing data but not the content of the message or the payload, but could span to access to the actual payload, the message content. And PHI could be involved in both data scenarios. You definitely need policies on that in my regard, and whether those are properly enforced through business associate agreements or a combination of very clear BAA requirements and some other governance functionality, and John, I'm sure you can get on your soapbox here, we should talk about.

Then I'm a lot less comfortable with number five, because to me there's a lot more that's involved here. But again, we still are assuming a scenario that is direct or one to one and not one that involves, for example, a database model, which I listed as another scenario, or a query and response type model where you don't have the data holder in a strong role and vetting whether the request is one for which the data ought to be released. I'm going to stop there, because I've just been talking a lot and there's a lot in here to talk about, and I want to open up the floor for comments and folks' reactions to this.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

I just wanted to get a definition of data holders to make sure who could be doing this push and vetting the appropriateness of the recipient.

Deven McGraw - Center for Democracy & Technology – Director
I think we're still talking about stage one of meaningful use, because that's been the locus of our discussion to date. So we're talking about the eligible provider or the hospital who's exchanging data to meet stage one of meaningful use.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
And whatever recommendations would come out would clearly state if the data holder were other types of covered entities, that this consideration would have to be redone because of different relationships to the patient and their standing for making those kinds of vetting decisions. An example from the meeting last Friday was what if the pair were pushing PHI directly to another provider, a provider in their network.

M
For what purpose? Was it still treatment payment or health care operations person?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It was operations.

Gayle Harrell – Florida – Former State Legislator
This is Gayle. I want to comment on that.

Deven McGraw - Center for Democracy & Technology – Director
Okay, I'll go to let you comment. My answer to the question is that I think it's easier to address this for a defined set of circumstances and then test that against others if we're able to and we have time. I think it's limited to stage one, because I think if we get through that and then we can test some other more common scenarios and see if it still holds.

M
So you're saying stage one provider to provider.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

M
Okay.

Deven McGraw - Center for Democracy & Technology – Director
There is a stage one provider to payer on an eligibility check for meaningful use.

Gayle Harrell – Florida – Former State Legislator
That's the scenario that was discussed at the policy committee meeting – this is Gayle – then come into play where you have a payer pushing to a provider.

Deven McGraw - Center for Democracy & Technology – Director
Remind me, Gayle, in what context?

Gayle Harrell – Florida – Former State Legislator

In what context it's talking about the prescription drug issue on the payer pushing information, basically medication history, to another provider from a mental health drug.

Deven McGraw - Center for Democracy & Technology – Director
Right.

W
And that needs to be differentiated from the provider to payer transactions that are already governed under HIPAA for payment.

Gayle Harrell – Florida – Former State Legislator
Correct. I don't know, when it comes from payer to provider, is that covered under HIPAA?

W
This particular one is not a HIPAA covered transaction that you're talking about Gayle.

Paul Egerman – eScription – CEO
I think an important distinction we need to make here is that payers will say that certain things that they do are not considered payment functions, that they will actually perform functions that they believe are treatment in nature, such as care planning, disease management, and stuff like that. That's something that needs to be considered in all of this.

W
That's a big issue because the definition of treatment never puts the payer in the driver's seat, as far as I can tell. It's always the provider who has to initiate those kinds of relationships for care coordination.

Deven McGraw - Center for Democracy & Technology – Director
I think we ought to, for the sake of being able to draw some recommendations that are most helpful to the scenario that is most on the horizon, which is stage one of meaningful use financial incentives, and so that does not govern the payers pushing data to physicians per current HIPAA rules which cover them. What it covers is whether the provider for stage one of meaningful use in a direct exchange environment needs to get additional consent to the patient in order to perform any of the exchange functions that are part of stage one of meaningful use.

M
I think we still have to be a little bit careful here, because I understand that the focus is on stage one meaningful use, but if we know that payers are currently performing a whole variety of functions that they will lead to be treatment related, I don't think we can bury our heads in the sand and say we just don't want to consider those. Because they're happening today, they're going to happen with higher frequency, and we have to take those into consideration, unless I'm misunderstanding how you're going to deal with those.

Deven McGraw - Center for Democracy & Technology – Director
No, John, none of this is bury our heads in the sand. I'm asking us to deal with these issues in manageable chunks. So, I don't doubt that we have some interesting issues that we could grapple with, with respect to how data flows for treatment payment and operations generally, it all happens without patient consent, but we started this conversation looking at whether additional – … large we want a trust framework that applies to all of those things. We, I think, will talk and talk and talk and not be able to come to conclusion if we don't try to settle this in bite size chunks.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. I agree with you. Can we just have a parking lot for some of these issues that John just brought up? Because at the end of the day consumers are not going to understand why their data is treated one way with exchanges from the payer to the provider and treated another way if it's stage one meaningful use and they're starting to see some more control of trust framework there. So they need to see it across the board. We know we have to take it in chunks. But if we know that there's a parking lot for these issues I would be happy.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Paul Egerman – eScription – CEO
This is Paul. I do think consumers know who their physician is, however, or who the hospital is and they know if they've given their consent for the physician or hospital to do something. Consent for insurance companies is a totally different ballgame.

Deven McGraw - Center for Democracy & Technology – Director
Absolutely.

M
Just one other thing when you parking lot that, I don't think payers are considering this treatment. I think that they've taken a position that it's not treatment and it gets into the whole malpractice thing. They haven't crossed that line, that's my understanding.

Mike DeCarlo – BlueCross BlueShield
That would be correct. This is Mike DeCarlo with …. If payers are engaged in operations through ePrescribing or providing medication histories or are assisting physicians with care coordination it is considered operations and not treatment.

W
That's the definition of operations. Again, the provider has to be the instigator, not the payer.

Paul Egerman – eScription – CEO
I think we're painfully close to this edge here, I really do. I'm not sure that's universally agreed or accepted.

Deven McGraw - Center for Democracy & Technology – Director
All right, you're not sure what's universally agreed?

Paul Egerman – eScription – CEO
That it's operations. Again, I'm very happy to parking lot this one as long as we recognize that it's something that we are going to need to deal with.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Okay, totally agreed. I don't think we've ever taken anything off of our table in a permanent way.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. If you're going to go down your list I would like to highlight if we put blinders on and say this is just direct push. And looking at number four, where the intermediary has some adding some value and it actually has access to the PHI, if we have blinders on to say this is just point to point

provider vetted transactions we may forget that once this intermediary has this data available, what is to keep that intermediary from turning around and using it in a query scenario where the requester is a provider who has particularly no relationship with the patient or some other entity participating in the HIE. So—

Paul Egerman – eScription – CEO
They're contracts in the law.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I think we need to be very careful when we get to that place about what happens with that data once it's stored.

Deven McGraw - Center for Democracy & Technology – Director
Yes, so that's why and what I had said in scenarios one through four was that in each instance there needed to be very clear policies in place that place limitations around the use, reuse and retention. Whether that best happens through a business associate agreement or whether that's actually better enforced through other mechanisms or through a combination of mechanisms in my view is never off the table—

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
The only issue that—

Deven McGraw - Center for Democracy & Technology – Director
I'm almost done, Kathleen. Essentially, what I was getting at is that a lot of this stuff is very arcane to patients, some of these functionalities that an intermediary might do in one through four, and so patient consent, therefore would be a pretty weak policy prescription for dealing with that, and that it would be more ideal to have some very clear rules that were enforced that would limit the use, reuse and retention of that data. Now, having said that, you just made me think of something, Kathleen—

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I'm fine. ….

Deven McGraw - Center for Democracy & Technology – Director
… if it's not in place that I might be inclined to give patients more of a role in saying I don't really want my data exchanged through this thing because there are just not enough controls on it.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
All I'm saying is what's missing between four and five, we need a home for the idea of the data being available for the full model or the query model and it's not in either, so that was my ….

Deven McGraw - Center for Democracy & Technology – Director
Yes, I put the query model down in number seven, because I assumed that one through five were all directed push.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Okay.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Deven, I'm sorry. I can't find what you're referring to, one through five from.

Deven McGraw - Center for Democracy & Technology – Director
There was a discussion guide that Judy sent in an e-mail on Friday.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
About business associates?

Deven McGraw - Center for Democracy & Technology – Director
No, it's another document that was in that same e-mail.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Oh, I didn't see the second one. Okay, fine. Thank you. I'm sorry to interrupt.

Deven McGraw - Center for Democracy & Technology – Director
That's okay.

Gayle Harrell – Florida – Former State Legislator
I just have the HIPAA thing. I don't have anything else. This is Gayle.

Deven McGraw - Center for Democracy & Technology – Director
You should. It was all in the same e-mail.

Judy Faulkner – Epic Systems – Founder
I'll resend it to Gayle and Dixie right now.

M
… recommendations.

Deven McGraw - Center for Democracy & Technology – Director
Yes, it's called "Recommendations." Thank you. Go ahead, Marianna.

Marianna Bledsoe – NIH – Deputy Associate Director
I have a question about one of the assumptions. It says it applies to individually identifiable information and you've said that we'll have to consider at a later date rules for data that's considered to be de-identified under HIPAA. But what about limited data sets?

Deven McGraw - Center for Democracy & Technology – Director
That's identifiable information.

Marianna Bledsoe – NIH – Deputy Associate Director
Right, so would we consider those in the same way through these scenarios?

Deven McGraw - Center for Democracy & Technology – Director
Again, since we're limiting it to stage one of meaningful use I think you have to think of which of those criteria are going to trigger a limited data set. So that would include anything on public health where a limited data set gets used to respond to a public health reporting requirement. That's the thing that jumps out. You had said you thought there was research and then I guess maybe on the reporting of the data to CMS, but even in that case I'm not sure if folks would use a limited data set to do that.

Marianna Bledsoe – NIH – Deputy Associate Director

I think there was one, and again, I’m not sure that folks would use them to generate lists of patients either for research. I suppose there could be a generation of a list of subjects for the purposes of identifying whether or not, for example, there might be enough patients to enroll in a particular study.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I don’t see any of that in the meaningful use criteria.

Marianna Bledsoe – NIH – Deputy Associate Director
There was a reference to patient lists, and I know I was supposed to send something on this. Maybe that’s –

Deven McGraw - Center for Democracy & Technology – Director
Yes, from the meaningful use workgroup, that’s an internal list of patients that’s intended to be used by the provider for care management purposes. It wasn’t intended to be research use, at least for stage one. If providers then use that list for research purpose they’d have to follow HIPAA rules and the common rule if it was federally funded.

Marianna Bledsoe – NIH – Deputy Associate Director
I understand. I’m just trying to see how this might be relevant to some of those uses.

Deven McGraw - Center for Democracy & Technology – Director
I appreciate that. But I’m struggling with where it comes up or where it would make a difference if it did.

Judy Faulkner – Epic Systems – Founder
Could I ask another question about one of the assumptions, and that is the assumption that the patient can select the PHR. I don’t really know what that means. Let’s assume there are 300 different PHRs out there and someone has half a million patients, can any patient choose any PHR and then what does the EHR have to do to get that patient’s data over?

Deven McGraw - Center for Democracy & Technology – Director
Here’s the context in which that arose, and let me see if this makes sense. We said that exchange for stage one of meaningful use if it was direct wouldn’t necessarily require any greater patient consent than would be the case under current law. Now, there are meaningful use criteria that involve exchanging data with patients and so there’s a built-in assumption there that data exchange with patients is of course done with patient consent and that if in fact that data is sent somewhere it would only be sent somewhere if the patient indicated that it ought to be sent there.

Judy Faulkner – Epic Systems – Founder
So you’re not saying that the EHR has a responsibility to send it to anything the patient chooses, you’re just saying that if the patient chooses consent is assumed.

Deven McGraw - Center for Democracy & Technology – Director
That is what I’m saying, although I’m struggling with the –

Judy Faulkner – Epic Systems – Founder
Which ones, the first or the –

Deven McGraw - Center for Democracy & Technology – Director
The first part of it, only because I think what I wanted to make very clear here is because we’re dealing with whether additional consent ought to be required we don’t want to have a scenario where somebody

wants to check off the box of exchanging data with a patient by sending it, for example, to some PHR that the patient never authorized. In other words, if you assume that patient consent is present, any time that the data is being sent to an individual you have to assume that the individual has agreed that it's going to a particular PHR and not being sent without that agreement. I don't think we meant that out of the 300 PHRs out there if the patient chooses Annie's PHR Shack and Epic doesn't interface with that, that they'd be in trouble. That's not what I meant when I put that down.

Judy Faulkner – Epic Systems – Founder
Okay, fine. Because I do think some of the PHR vendors believe that every EHR must interface with them, and that's weird.

Deven McGraw - Center for Democracy & Technology – Director
Yes. Other thoughts? And for those of you who didn't get a chance to read this, I'm sorry about that, because it really is important to the discussion, but essentially are folks comfortable with the notion that for scenarios one to three we wouldn't put additional consent requirements on direct exchange, but we recognize that in each case the intermediary isn't accessing some data and there need to be clear rules around that better enforced. With the mechanism of enforceability a little bit of an open question, whether that's best done through the business associate agreement or through some other rules through which there would have to be some accountable authority, governance to enforce that. Spending conditions enforced by ONC might be one mechanism, but I think there's a whole host of issues that come up under the governance category that the NIHN workgroup is going to have to very soon tackle.

W
I want to ask, you're including number three where you're saying the intermediary has some access to metadata and to payloads for limited reasons.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

W
Define that a little bit more. I'm not sure I understand what you're saying there. If they have no access, if they're simply transiting stuff and they never open the suitcase, if you have a suitcase and you're just transiting it, that's one thing. Then you have to –

Deven McGraw - Center for Democracy & Technology – Director
Right, so under what circumstances would that suitcase have to be opened to perform some minimal functionality? That's a good question, and I could ask folks from the – I was in communication with Arien Malec and David McCallie about this.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Deven, this is Kathleen. The … direct transport in the metadata can include comments and indications in the file name as to what type of data is going over, and it can be PHI. So there's no guarantee that the metadata itself will be PHI free.

Deven McGraw - Center for Democracy & Technology – Director
That's absolutely right, Kathleen. Number two talks about the access to metadata and it sometimes could be PHI, but I thought that Gayle's question was not about the label on the suitcase that might be quite extensive, but the payload. That under what circumstances would an intermediary or even some sort of core set of internal operations and making sure their quality of service is up to snuff, would need to be accessing the payload.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I would agree with that question.

Deven McGraw - Center for Democracy & Technology – Director
Yes, it's a very good one.

W
I have a real issue with that.

Judy Faulkner – Epic Systems – Founder
Who is the intermediary? Maybe you … and I missed it.

Deven McGraw - Center for Democracy & Technology – Director
You.

Judy Faulkner – Epic Systems – Founder
If the customer controls the software the intermediary is still involved even though the intermediary does not touch the software?

M
Touch the data, you mean?

Judy Faulkner – Epic Systems – Founder
No, the software is under the control of the health care organization, it runs on their machines with their people.

M
But I think what they're talking about is two health care organizations and the data going between two health care organizations.

Judy Faulkner – Epic Systems – Founder
Right, so the intermediary is the owner of the software?

Deven McGraw - Center for Democracy & Technology – Director
No, this isn't an issue of ownership, Judy. It's an issue of –

M
Transaction service.

Deven McGraw - Center for Democracy & Technology – Director
Yes. When you're providing a service that moves the data from point A to point B what data do you have access to, to make sure that transport happens?

Marianna Bledsoe – NIH – Deputy Associate Director
Judy's point I think is whether it's intra or inter-enterprise. If it's intra I don't think that's what we're discussing.

Judy Faulkner – Epic Systems – Founder
Yes, so –

Deven McGraw - Center for Democracy & Technology – Director
If it's in an institution, no, outside of the institution's law.

Judy Faulkner – Epic Systems – Founder
The question is really if the software is under the total control of the institution itself sending it or releasing that. I like your word there releasing, because it's not always sending, sometimes it's just releasing or supplying it. It's under the total control of the health care organization who uses the system to say can I send this? Yes, I have the signature. Yes, go. Push it, it's now released, and it's there to pick up by the other one. Is there an intermediary?

M
I think there is if they are two different providers, two different tax IDs, two different databases.

Judy Faulkner – Epic Systems – Founder
In other words, the intermediary is the writer of the software, even if the writer of the software has left the hovering over that and is not involved with what goes back and forth.

M
Yes.

W
I still haven't gotten the …. Can the intermediary be a business associate?

M
They're supposed to be.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

M
Yes, I think so.

Paul Egerman – eScription – CEO
This is Paul. To get back to Judy's question, maybe I'm misunderstanding this, but I assumed scenario number two was more like I'm a small group practice and I want to send or receive laboratory orders, and rather than send it directly to a lab I send it to my handy-dandy local regional HIE. And it says oh, you want to send something to, say, Quest Laboratories, and they re-package it and send it to Quest, and then Quest sends it back unresolved and they just re-package the result and send it to me, without reading the results, but they have a little bit of information along the way. So they're an intermediary, but they're just helping deliver the message. Is that scenario number two?

M
I think that's right, all the same thing between two providers.

M
It could be …

W
… either.

Judy Faulkner – Epic Systems – Founder

The analogy is if I send you an e-mail is Microsoft, because I'm using Outlook, the intermediary?

M

No, it's your network provider that's the intermediary.

Paul Egerman – eScription – CEO

I'm not even sure that that's – the only reason why the HIE is an interesting intermediary is it does have to read a little bit of the metadata. In other words, the assumption is that the small group practice doesn't have the ability to send directly to the laboratory so HIE helps it, or it doesn't have the ability to send from a primary care provider to the specialist. So the HIE is an intermediary and it reads something in it, the message, to figure out where it's supposed to go and has its own set of rules and maybe you had to set up something very individual for each one to try to figure it all out based on the version of software you're using or based on all kinds of stuff.

M

To format it so that the other provider can actually receive it.

Paul Egerman – eScription – CEO

Yes, so it's doing a little bit more than a Microsoft Exchange server or something. It really is accessing some of the metadata and …

W

In other words, it's opening the suitcase.

Deven McGraw - Center for Democracy & Technology – Director

But data is on the suitcase label.

Judy Faulkner – Epic Systems – Founder

But, Paul, if it is an EHR vendor that has a facility built into it to say you can ship the data but doesn't monitor that at all, I mean, doesn't get involved with that and … add an intermediary. Because I think that's what the EHR vendors on the whole are going to end up doing.

Paul Egerman – eScription – CEO

Then they'll be intermediaries.

Judy Faulkner – Epic Systems – Founder

That goes back to the Microsoft analogy.

Paul Egerman – eScription – CEO

I don't see the EHR vendors being the intermediaries unless they're running their own Exchange network.

M

Some of them do, though. Some of them have hubs that integrate with other EHRs, and they're acting as intermediaries.

Paul Egerman – eScription – CEO

The basic assumption here, Judy, is that the intermediary is involved in every single message. They're not just providing software to handle the messages; they're actually handling the messages themselves. They are the letter carrier, as it were.

Judy Faulkner – Epic Systems – Founder
Okay.

M
Yes.

Paul Egerman – eScription – CEO
I don't think that's, I don't know maybe it is, but I don't think that's true of most software vendors. They're not the letter carriers. They do other things, but they don't actually carry the letters themselves.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
There are instances of that.

Paul Egerman – eScription – CEO
There are some, but I'd say most of them do not.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I think the criteria is whether they have to have a business associate agreement in place, would probably be ….

Deven McGraw - Center for Democracy & Technology – Director
Right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie Baker. I finally got the scenarios and I have another one that's a real case that I recently came across and I think it fits into this. A provider wants to send the data, pure PHI, to an intermediary for strictly the only thing the intermediary does is de-identify the data.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
They have to look at the PHI to do that.

Deven McGraw - Center for Democracy & Technology – Director
Right, and they'd have to be a business associate in order to do that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This brings up another point, which is if they are able to do that is that de-identification function in which one of these scenarios? Is it four or five?

Deven McGraw - Center for Democracy & Technology – Director
It's not in any of the scenarios, because we're trying to limit the discussion to the scenarios that pop up under stage one of meaningful use –

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
… neither, so we have mentioned –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I thought that did come under stage one. It seems to me that the only thing, and I'm not a lawyer, the only thing a business associate does is de-identify data so that providers can send it to a research institution, let's say, or something, or a pharmaceutical company or something. That seems to me to be

an exchange between the provider and the pharmaceutical company. It just seems, to use Paul's example from last week of the expectation, I don't think patients would think that their provider is sending their identified data to somebody just to de-identify it. Because they do have the entire record in order to de-identify it, and if that's the only –

Deven McGraw - Center for Democracy & Technology – Director
Dixie, I'm going to stop you, only because we have de-identified data in the parking lot. I don't want to take it up here, because we need to come to this initial set of recommendations on exchange for stage one of meaningful use.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
… sit there. I'm sorry. I thought –

W
There is de-identified information, I believe, that goes in public health …

Deven McGraw - Center for Democracy & Technology – Director
It's not always de-identified. In fact, it's not required to be de-identified before it's sent. Whatever is the particular public health requirement by law, that's what gets sent. In fact, patients can't consent around that.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Right. And Deven, once they agree to let an intermediary have it for the purposes of de-identifying it, then the intermediary can do all sorts of things with that de-identified information.

Deven McGraw - Center for Democracy & Technology – Director
That's right. But to me that triggers more of the more robust conversation I want to have about what people can and can't do with de-identified data and protections against re-identification that we don't have. That's why I –

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Can we just leave –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
She's saying it's in the parking lot. You just don't think it's stage one …

Joyce DuBow – AARP Public Policy Institute – Associate Director
This is Joy. I think it would be very useful – there are a lot of topics that are being discussed and a lot of these perspectives are just very interesting. But we need to impose a little bit of structure on this conversation in order to make a little bit of progress. I think what Deven has asked is one way of proceeding, if you have another way of proceeding to support some kind of structure here to reach some resolution on some of this, then that's okay. But if you don't, let's try to adhere to what Deven's trying to do here which is go through this at a very basic level and then you can add on some of these issues that you're raising.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. That to me is fine. But the issue is if you say we're fine with level four, no consent and then we introduce de-identification as one of the capabilities for that in a type of intermediary, would we have made the decision we made previously that we were comfortable with level four being without consent.

Deven McGraw - Center for Democracy & Technology – Director
Right, and I suspect that some of us would not when we add that in, when we start to pressure test this model outside of the context of the stage one, the exchange that's required for stage one of meaningful use.

Joyce DuBow – AARP Public Policy Institute – Associate Director
If you find that you're saying that you think that some of the stage one requirements are more complicated than are reflected in the assumptions, then let's scale it back to where you are comfortable but you're at the bare minimum and work from there.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I know that biosurveillance reporting sometimes uses de-identified information, and I think we should list it as five and leave the discussion about what should be done with de-identified information in the parking lot, but at least list it in the model.

Deven McGraw - Center for Democracy & Technology – Director
I think what I would prefer to do is to – I think we can have models and I think we can also, to the extent that we have some issues that we think we can't necessarily leave in the parking lot because they are inherent to making decisions on the model, is to say where one of the functionalities, for example, in some of these more robust intermediary examples of four and five includes de-identification, it doesn't make us comfortable because we have some issues that we need to resolve there.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
That would be fine with me.

Deven McGraw - Center for Democracy & Technology – Director
Yes, okay, which I get. I totally get that. We had a lot of conversation about this on the last call too.

W
Could we go through these point by point, start with one, start with two, go to three, and say yea or nay and specifically why yea or nay one by one.

Deven McGraw - Center for Democracy & Technology – Director
It's not a bad idea, although I think we might be able to chunk one and two because if the letter carrier is getting access to any data at all it's just what's in the envelope or the message or the metadata. Notwithstanding that we would not want unlimited use of that, because Kathleen is right, that's sometimes PHI.

W
Who is going to determine what those clear limits of use, reuse and retention are?

Deven McGraw - Center for Democracy & Technology – Director
We can make some suggestions in that regard.

W
Because I think you have to know that before you can say yes, and I think that has to be extremely clear, either in a governance model. I'm not sure that business agreement is strong enough.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I was thinking about that too.

W
Because those are contracts between business entities, and let me tell you I know a lot of people who breach contracts and you don't have much recourse other than in a civil suit.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Except that business associates now, thanks to ARRA, are regulated.

Deven McGraw - Center for Democracy & Technology – Director
You can be held more accountable, but it still is going to be dependent on, I think there are some other issues that we'll talk about in terms of whether we think that the business associate agreement is the right vehicle for imposing these requirements. Because as you may have seen if you had a chance to read the summary that Adam did for us, it leaves a fair amount of discretion to the contracting parties and doesn't require it to specify, at least as of today, anything in particular beyond you're never allowed to access user disclosed data beyond what you could do under HIPAA. But I think that's a broader universe than I suspect a lot of us would be comfortable with, with respect to an intermediary in the middle.

Paul Egerman – eScription – CEO
But the real issue is not how good or bad business associate agreements are. The real issue is based on the existence of business associate in scenario number two, what should the consumer choice be, right? Isn't that the real issue we're trying to solve?

Deven McGraw - Center for Democracy & Technology – Director
It is the real issue we're trying to solve. But I think I'm with Gayle here, which is that I can't get to the place of saying – I don't think it's important to layer on more consent than is already required in law unless I know that there are some other strong rules in place.

Gayle Harrell – Florida – Former State Legislator
Right, exactly.

Deven McGraw - Center for Democracy & Technology – Director
Quite frankly, if we are defaulting to the patients to hold up the privacy protections for transport through an intermediary, we're probably not in a very good place.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. I like Gayle's idea about going through where we have an issue with each one of those.

Deven McGraw - Center for Democracy & Technology – Director
Okay, that's fair.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I would kick off on number two with the idea that given what we got from OCR and the lack of clarity about – I guess what I want to say is what a covered entity might choose to do and their interest in doing some of the activities that were in the OCR paper that we got, they would have much less interest in doing that than an HIE who has to have a sustainable business model. So where a provider would not have a great interest in storing a lot of the metadata or some minor pieces of the payload to do other things with, because it's not in their business model, an HIE might have that interest and I think that is the point at which the business associate agreement starts to be problematic.

Deven McGraw - Center for Democracy & Technology – Director
Yes, okay.

Adam Green – OCR
I wonder if it also would be worth separating two out depending on whether or not the metadata includes individual items … health information. Because if it does not, then you're probably not looking at a business associate relationship, there would be no business associate protections there under HIPAA.

Deven McGraw - Center for Democracy & Technology – Director
Is that a fair assumption for the group, that if in number two the metadata contained no individually identifiable health information, would folks be more comfortable?

Adam Green – OCR

One example of that is that there’s talk about trust enabling organizations whose sole purpose is to verify providers and say yes, this particular provider is who he or she says he is. They may not have any access to the patient information.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. I think that’s highly unlikely not to have the payload. When you look at the standards that they use to move this data, there’s a part that’s called a content type which describes the type of payload. And if they don’t know the type of payload they don’t know how to route it. It would be probably pretty hard to dictate that the comments and the final names weren’t to include any PHI. So the trust organizations probably will want to be doing both. I don’t think you’re going to see them decoupled. It may be possible, but it’s not likely, from what I’ve seen done in the industry.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think if we just called it the messaging metadata that would be clarified, because the payload has metadata too, but if you’re talking about the messaging metadata you’re talking about HL7.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
The messaging metadata in some of the standards does include a content type description in the envelope.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Right, but that’s not PHI.

W
… a better definition of content type, for instance, lab results, medication, history, what?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It has a comment field where they can put anything they want, there are no restrictions, and it can include a file name, that can include the name of the patient for the file and the type of file that it is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, that’s true, ….

Gayle Harrell – Florida – Former State Legislator
The type of file, but no information that resides within the file.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
She’s saying if they name the file something like “GayleHarrell.com” ….

W
Gayle Harrell … PDF.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
And they can have comments that can be free form, there’s no restriction on it. So if Adam’s correct that there are entities that are only going to do the authentication of the providers and that kind of directory service, that would be fine. But I just don’t see them having enough value add for anyone to even use them if they’re not also routing that data.

W
Kathleen, I have a question for you. We’re talking about the message header, is that right?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager

There's payload that gets wrapped by different levels above it that are considered routing or metadata kind of information.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, header, that's what she's talking about.

W
That's what I meant by metadata, but clearly if there's metadata also in the payload. I meant the message content.

W
So for the message content, the routing information, would it be necessary for a provider to indicate whose information was inside in order for the recipient to know where it went, or not?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Not.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It's not necessary. There's nothing in the standard that precludes it. You have to indicate what kind of payload format you've got so they know where to route it.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
… and I think that we can almost put that as operational practices. A header for a message shouldn't have PHI. But what she's saying, and she's right, it could. But shouldn't we put that in the realm of smart operational practices?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
Well, it's also one of the factors, I think you're saying, that you would want to consider, that you would consider messages that have no PHI in the routing information perhaps differently than you would consider messages that have PHI in the routing information.

W
Just having that differentiation may be enough to change the operational practices, as Dixie is stating, to limit PHI so that they don't have to have any kind of business associate agreement, like Adam was pointing out.

Gayle Harrell – Florida – Former State Legislator
I think that would meet a standard, if you say that the routing information did not include PHI. I think that could be acceptable when you –

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
And you wouldn't have to change the standard, you'd just say if this entity is going to send it without … of any PHIs, they're doing other value adds like provider directory, then they don't have to have a business associate agreement. If they do, using the same standards, not limit what's in the metadata then they do have to have a business associate agreement.

W
Right.

Deven McGraw - Center for Democracy & Technology – Director
This has been very helpful. So in number three I thought I heard Gayle say they should just not have access to payload.

Gayle Harrell – Florida – Former State Legislator
Correct.

Deven McGraw - Center for Democracy & Technology – Director
Yes, I'm curious as to why they would need to as well for basic functions, unless they were exploring a business model that involved providing an enhanced set of services where they actually needed the content.

Gayle Harrell – Florida – Former State Legislator
That's … four.

Deven McGraw - Center for Democracy & Technology – Director
Yes, which is really in four, so maybe there isn't – I can raise that question about why that even needs to be a separate option. Once you trigger into payload access, number one, you're absolutely in business associate agreement land. Number two, what types of functionalities are we comfortable with before it passes over to the point where we think there ought to be, maybe there's an additional role for consumer consent.

Gayle Harrell – Florida – Former State Legislator
Deven, I think that I was given an example of this at one point and I would like the technologically oriented people on the phone to see if I'm right and this is an example of three. There are times when a message might bounce, for some reason, because of the way the information was formatted in the payload and so that the intermediary would need to open the envelope to see what the problem was, reformat, and then resend.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
That is true. There's also, with respect to three, you have to look at this in terms of the standard that you're considering. So if you're looking at an X12 transaction, they have to get into the payload to find the routing information because the X12 transactions don't carry enough in their envelopes.

Gayle Harrell – Florida – Former State Legislator
Kathleen, can you stop a minute and explain to people what an X12 transaction is.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
It would be the typical ones used for the HIPAA transactions like claims.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Eligibility and all that. I'd like to propose that we not use the term "metadata." Because both the payload has metadata and the envelope does too.

Deven McGraw - Center for Democracy & Technology – Director
Yes, that's fine, Dixie. We can do that.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
… payload versus ….

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I was agreeing with Joy with respect to certain transport standards.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes.

W
I think, again, if it's an EHR, releasing that information is left to the customer to figure out how to do it. It's the customer who will get in and look at the data. The EHR vendor wouldn't be involved at all.

M
That's correct.

Deven McGraw - Center for Democracy & Technology – Director
Well, and I don't know that we're talking at this level about an EHR vendor as the type of intermediary that we're talking about. I think we've moved into a function that a clearinghouse might provide, for example, or what the NHIN workgroup is calling an HISP.

Judy Faulkner – Epic Systems – Founder
But, Deven, I think there are some EHR vendors who act as an intermediary for one or more customers in this way. They just need to be called out as acting as a business associate ….

Paul Egerman – eScription – CEO
This is Paul. I think really we need to define what an intermediary is. An intermediary is somebody that's not the health care organization, that's actually transporting transactions or messages.

Judy Faulkner – Epic Systems – Founder
I guess that's what the word "intermediary" is, needing a real good definition. I'm sorry, Paul. Go ahead.

Paul Egerman – eScription – CEO
Yes, but it's somebody who's actually transporting the message. Some vendors do that. Most vendors don't, but as you define that, I think that that solves that issue. If Judy didn't understand it, I imagine a lot of other people won't also.

Deven McGraw - Center for Democracy & Technology – Director
Okay, that is fair. The problem is we've used intermediary to be all sorts of things.

W
Yes. It's our placeholder.

Deven McGraw - Center for Democracy & Technology – Director
Right. So maybe we need to have intermediaries that are acting as clearinghouses and adding value differentiated from transport types or not working type intermediaries.

M
I wouldn't use clearinghouse, because of the connotation with all of the HIPAA payment transactions. I'd use another term.

Deven McGraw - Center for Democracy & Technology – Director
Okay.

M
Because clearinghouses are a covered entity under the HIPAA framework.

Deven McGraw - Center for Democracy & Technology – Director
Right.

M
So don't use that term.

Deven McGraw - Center for Democracy & Technology – Director
Yes, but I think sometimes they will essentially be clearinghouses under HIPAA because the technical definition of a clearinghouse is an entity that transforms unstructured data into structured data, right?

W
Yes.

Deven McGraw - Center for Democracy & Technology – Director

So it doesn't necessarily have to be changing it into the HIPAA code set so that a payment transaction ….

W
It has to be a transaction that's covered under HIPAA for it to be a HIPAA clearinghouse.

Deven McGraw - Center for Democracy & Technology – Director
Okay.

W
There are generic clearinghouses, but maybe for the purposes of this discussion we could say "value add intermediary."

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
VAI.

Deven McGraw - Center for Democracy & Technology – Director
Just what we need, another acronym. All right, so I think what we keep running into here, and we're going to have to open up this call soon to public comment, is so now that we've come up with this term, at least temporarily if not for a longer term, of the value added intermediary, what are the value adds done by an intermediary that, number one, trigger some level of concern where we think, you know, we ought to require patients to either opt-in or opt-out of them, versus putting up a set of very clear policies that place some very clear parameters around the value add services. So that essentially those services we understand that there's a need for them in the marketplace but we're not opening up the Pandora's box where they're getting data, for example, for a clearinghouse type function or a data transmission function but they're using it for a whole host of others.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
This is Kathleen. One criteria that strikes me is whether the value added service is specifically for the benefit or on behalf of the covered entity who has made this decision on behalf of the patient to send the data, versus value added services that are available to other participants in the HIE or participating in this value add intermediary or to external entities.

M
That confused me.

M
It was actually pretty good.

W
Yes, I liked it.

M
So in other words, is it just for the covered entity that's sending the information, or are there other additional services?

W
Are those services for the benefit of the covered entity who was sending the data?

W
Are they for the benefit of the covered entity, or the benefit of the patient?

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I think it all depends on how you define benefit of the patient. If you were to assume that – so let's say for the benefit of achieving meaningful use, do you consider meaningful use to be patient-centered? Sometimes it's populations of patients, sometimes it's individual patients. But those are the criteria that we're focusing on. It enables the covered entity to facilitate the meaningful use transaction.

W
I like that because it limits some of the somewhat broad areas where a covered entity under HIPAA can do things that may be beyond meaningful use, like marketing or some ….

W
Correct, that's exactly where I was going with the benefit of the patient.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
I agree with you.

Mike DeCarlo – BlueCross BlueShield
I think the meaningful use is a very narrow straitjacket for some of the uses of this information. It may still be in the patient's benefit. Can we go back to what we discussed at the last meeting about the reasonable expectation of the patient and how this information is going to be used for their benefit? That's a little broader, but it's still based on the patient's understanding of the information that they're turning over when they present themselves for services, with the expectation that services will be provided and the information they're turning over will be used for their benefit to receive those services.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
John, this is Kathleen. Under the meaningful use …

Deven McGraw - Center for Democracy & Technology – Director
That's Mike.

Kathleen Connor – Microsoft Health Solutions – Principal Program Manager
… broader sense is there anything that's missing out of that mix that you see? Research and population health and all of those things seem to be part of meaningful use, so I'm not quite understanding what would be more than that.

Deven McGraw - Center for Democracy & Technology – Director
Mike, I get what you're saying. I think, first of all, there's not very much on research in meaningful use, and research is covered by a specific set of rules and it's yet another issue that I'd love to put in the parking lot. But I'm trying to think about a way to – what I'm worried about in the patient expectations frame for this, is that I think ultimately that's our overarching frame for all of our discussions. But I'm worried that in terms of taking this in chunks we will spiral into a conversation about which uses under HIPAA writ large are within patient expectations and which ones are not. That's a bigger conversation, it's a valuable conversation, but in terms of when we really focus this, for the time being, on stage one of meaningful use, then I think again we can pressure test it when we've got a set of core recommendations that we're comfortable with by adding on certain functionalities using the patient reasonable expectations test. Does that make sense?

Mike DeCarlo – BlueCross BlueShield
It does. My concern here is that we not do what we said we were not going to do, which is try to rewrite HIPAA regulations.

Deven McGraw - Center for Democracy & Technology – Director
Right. I think what we're really doing here is looking at using the meaningful use window of transactions for the new environment that providers are going to be moving into very soon, and starting first with that initial set of challenges and what we think the right trust framework is for that piece. Then I think it will be a lot easier to incrementally think about the other pieces of that. Does that make sense?

W
Deven, I have one more question before we let the public in. I was not on the first part of the call, I had another meeting that I was at, and forgive me if I'm going back over stuff you all went into. I know

Latanya had brought up the issue, and I wanted to clarify that we're talking about vetted access to this when we go direct exchange.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

W
In other words, the pinging that you're … about –

Deven McGraw - Center for Democracy & Technology – Director
We didn't quite get to the pinging.

W
… could not happen under the kinds of things that we're setting up … that that's the very premise when we start this.

Deven McGraw - Center for Democracy & Technology – Director
Yes, that's correct.

W
That this is only a direct push of information from one covered entity to another, that is covered under HIPAA and that the expectation of the patient is that the primary doc will be sending it to the specialist or that the hospital will be sending it to the doctor …

Deven McGraw - Center for Democracy & Technology – Director
Certainly with scenarios one to five they all assumed what I call directed or vetted exchange. Now, in the other scenarios that we really didn't get to talk much about, we talked about some other models that – I know I love the word "push" too. It's very hard for me not to use that word.

W
I like that because that says exactly how ….

Deven McGraw - Center for Democracy & Technology – Director
Judy will not let us use the word.

W
It's the reason it's going, somebody's requested it. The patient knows it's happening.

Deven McGraw - Center for Democracy & Technology – Director
Well, if the patient doesn't the provider does acting on the patient's behalf.

Mike DeCarlo – BlueCross BlueShield
I would say the patient's not surprised it's happening.

W
Right.

Deven McGraw - Center for Democracy & Technology – Director
Most of the time. All right, I'm going to try to work up some materials to advance this for our next call. But folks should, and this is my last comment before we open the lines up to the public, because we're really late, if folks want to send me some comments off line, especially those of you who didn't really get a chance to read through these scenarios in detail, please do so. Because Rachel and I, I think, are going to have to work with staff to do a lot of work in order to have a – our last call is our last call before the May policy committee meeting, so whatever we're going to try to formulate in recommendations we really have to have them teed up pretty tightly. I'll use all the notes from this call to construct them, but if you've got something you want to send me in the interim, please do. Go ahead, Judy, do your magic.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay, operator, would you please see if anybody from the public cares to make a comment. Deven, just a reminder that the next call is May 7th.

Deven McGraw - Center for Democracy & Technology – Director
Yes.

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Thank you. Thank you, Deven.

Deven McGraw - Center for Democracy & Technology – Director
Every once in a while we get lucky and we're able to end on time, even though we were late. Thank you all again for hanging in for this discussion. Again, feel free to call or send me information, because Rachel and I will try to get this very focused for the next call.

W
Thank you.

M
Thank you.

W
Thank you.

W
Goodbye.

Public Comment Received During the Meeting

1. Are you not saying that for a Trust framework: 1. Payload/Envelope header information should not contain PHI? 2. That the patient must have information that is understandable to the patient that allows them to be able to audit their consent direction (at whatever level of granularity/ opt-in or opt-out policy) has been followed in the transport and access of their data. 3. If an intermediately has access to any of the Payload/Envelope information including PHI, then the Following needs to be in place from a privacy and security framework to be trusted by the patient…. List

2. All of the discussion is related to the intermediaries potential access to the metadata or "the inside of the envelope". However, what security and privacy Framework is necessary for the Patient to be

comfortable that the Payload has gone to a provider that they (the patient) has approved or been accessed by someone the patient has approved?

3. Should there be language in anything related to a Trust Framework that identifies what information the patient can obtain about WHO has been sent their data and WHO has accessed their data? How does the Patient trust the Exchange Organization or Process without this as part of the security and Privacy Trust Framework?

4. When an intermediary is part of the transport of the HIE, then part of their actions will be identification and authorization of the providers that can and have access and are sent patient data. Does not any Trust Framework have to include some language that the provider directory information contains provider name, address, group practice relationship, etc. that makes the patient feel confident that they (the patient) can identify the provider who has received or access their records? Is not the same information needed for patient directed consent (and monitoring of such) going forward.